



# AIRLOCK WAF

— **Schützt Applikationen. Sicher.**

Airlock WAF schützt mit modernen und dynamischen Filtern unternehmenskritische, webbasierte Applikationen. Sie analysiert als zentrale Security-Instanz innerhalb des Airlock Secure Access Hubs jeden http(s) Request auf Angriffe und blockt somit jeglichen Versuch von Datendiebstahl und -manipulation. Im Zusammenspiel mit Airlock API und Airlock IAM besteht somit eine einzigartige Architektur für mehr Web-Applikationssicherheit.

## Einsatz von modernen Webfiltern

Airlock WAF analysiert jeden einzelnen Request zwischen Nutzern und Web-Portalen, -Anwendungen und -Services. Angriffsversuche werden blockiert, noch bevor sie auf interne Systeme zugreifen können. Airlock WAF bietet umfassenden Schutz gegen die OWASP Top 10 Schwachstellen sowie vor modernen Angriffen und ermöglicht das zentrale Management von Security Policies. Mittels modularen und innovativen Sicherheitsfunktionen bleiben Unternehmen den Angreifern immer einen Schritt voraus.

## Policy Enforcement Point

Im Zusammenspiel mit Airlock API und Airlock IAM wird Airlock WAF zum Policy Enforcement Point, der nur gefilterte, authentifizierte und autorisierte Zugriffe erlaubt. Diese Kombination von Access Management mit inhaltlicher Filterung garantiert kompromisslose Sicherheit.

## Security Dashboards

Das eingebaute dynamische und grafische Reporting bietet jederzeit Überblick über alle Angriffsversuche. Auch betriebliche Komplikationen wie Performance-Engpässe oder Back-end-Probleme werden erkannt, aufgezeigt und können mit unternehmensspezifischen Eskalationen oder Alarmprozessen kombiniert werden. Mittels interaktivem Drill-Down aus den Dashboards und dank der Anzeige der ursächlichen Logzeilen kann jeder Angriffsversuch exakt analysiert werden. Zusätzlich ist Airlock CEF zertifiziert, was eine Integration in gängige SIEM-Lösungen ermöglicht. Für Splunk steht sogar eine hausinterne Airlock Splunk App zur Verfügung.

## Plattformunabhängig, hochverfügbar und bedarfsorientiert

Airlock WAF steht als Hardware, Virtual Appliance oder als Cloud Image zur Verfügung und bietet somit höchste Flexibilität für alle Einsatzszenarien. Die leistungsstarke Airlock WAF kann im Bedarfsfall, z.B. bei saisonalen Business-Lastspitzen, problemlos zu einem aktiven WAF-Cluster mit mehreren Nodes ausgebaut werden. Der integrierte Load Balancer gewährleistet die geforderte Hochverfügbarkeit für Applikationen und Services im vollen Umfang und spart somit eine zusätzliche Architekturkomponente ein.

## Rundum flexibel

Durch effiziente und mächtige Konfigurationsmöglichkeiten ist vollste Anpassungsfähigkeit ohne Customizing möglich und zukünftige Updates werden zum Kinderspiel. Dank flexiblem Lizenzierungsmodell kann auf kundenspezifische Anforderungen eingegangen werden.

## Zentrale Security-Drehscheibe

Airlock WAF bietet viele Schnittstellen zu weiterführenden Systemen wie SIEM-Lösungen, Virenscannern, Fraud-Prevention-Systemen oder HSMs. Dank dem integrierten Threat Intelligence Feed reagiert Airlock WAF sofort auf aktuelle Bedrohungslagen aus dem Internet und schützt z.B. vor Bot-Netzen und anderen Gefahren, die gestern noch unbekannt waren. Über eine hochverfügbare ICAP-Schnittstelle lassen sich weitere Komponenten einfach anbinden.

## Deployment

Virtual Appliance, Hardware Appliance, Airlock Cloud Image

## Funktionen:

### — Eindämmung von Applikationsangriffen:

- Generische & spezifische Angriffssignaturen
- Cookie Store
- Request Validierung
- CSRF Tokens

### — Zugriffskontrolle

- Durchsetzungspunkt für Richtlinien
- Single Sign-on (SSO)
- Secure Session Management

### — Dynamic Whitelisting

- URL Encryption
- Form Protection
- Dynamic Value Endorsement (DyVE)

### — Policy Learning

- Automatische Regelvorschläge

### — HTTP(S) Reverse-Proxy

- Terminierung
- OCSP & OCSP Stapling
- Let's Encrypt Support
- HSM Integration
- Service Virtualisierung
- Content Rewriting

### — Hohe Verfügbarkeit

- Failover Cluster
- Load Balancing

## DevSecOps

Airlock WAF lässt sich dank eines umfangreichen REST APIs einfach in moderne DevOps-Prozesse integrieren. Bei der frühen Integration der Security in Entwicklungszyklen von Applikationen, auch in den neuen Docker-, OpenShift- und Kubernetes-Philosophien, bietet die Airlock WAF flexible Sicherheit. Erlangte Konfigurationen können auf einfachste Weise und somit effizient zwischen den unterschiedlichen Umgebungen transferiert bzw. eingesetzt werden. Auto-Learning- Mechanismen unterstützen beim schnellen Einsatz der Airlock WAF.

### — Logging & Reporting

- JSON Protokolle & Lucene query syntax
- Zugriffsstatistik
- Security Dashboards
- Performance Dashboards
- Troubleshooting Dashboards
- Kundenspezifische Visualisierung

### — SIEM-Integration

- Splunk App
- Common Event Format (CEF)

### — Threat Intelligence

- Webroot Feed Integration
- GEO Filterung

### — Konfigurationsmanagement

- Staging Support
- REST API

### — Cloud Image

- Kompatibel mit AWS, Google Cloud, Azure

### — ICAP-Schnittstelle

### — IBM Trusteer Pinpoint Integration

### — Schutz von MS Applikationen